Kapitel 8: Zugriffskontrolle

- Datenbanken enthalten häufig vertrauliche Informationen, die nicht jedem Anwender zur Verfügung stehen dürfen.
- Außerdem wird man nicht allen Anwendern dieselben Möglichkeiten zur Verarbeitung der Daten einräumen wollen, da Änderungen der Daten unter Umständen kritisch sind, auch wenn die Daten an sich nicht vertraulich sind.
- Zugriffsrechte können nicht nur einzelnen Benutzern zugewiesen werden, sondern es können Zugriffsrechte auch an *Rollen* gebunden werden.

Rollen

- `CREATE ROLE <Rollenname>`
- `DROP ROLE <Rollenname>`
- `GRANT <Rollenname> TO <Benutzerliste>`
- `REVOKE <Rollenname> FROM <Benutzerliste>`

Benutzer und Objekte

Jeder Benutzer wird durch die spezielle Kennung `PUBLIC` identifiziert; `PUBLIC` erteilte Rechte sind automatisch für alle Benutzer gültig.

- Zugriffskontrolle mittels `GRANT` und `REVOKE`.
- Objekte, die mit Zugriffsrechten versehen werden können, sind unter anderem Tabellen, Spalten, Sichten, Wertebereiche (Domains) und Routinen (Funktionen und Prozeduren).

Rechte

- Die möglichen Rechte sind `SELECT`, `INSERT`, `UPDATE`, `DELETE`, `REFERENCES`, `USAGE`, `TRIGGER` und `EXECUTE`, wobei nicht jedes Recht für jede Art von Objekten angewendet werden kann.
- Syntax:

```
GRANT <Liste von Rechten>
ON <Objekt>
TO <Liste von Benutzern> [WITH GRANT OPTION]

REVOKE [GRANT OPTION FOR] <Liste von Rechten>
ON <Objekt>
FROM <Liste von Benutzern> {RESTRICT | CASCADE}
```

- Mit `GRANT OPTION` erhaltene Rechte können weitergereicht werden.

Verwaltung von Rechten über Basistabellen

Der Erzeuger einer Basistabelle, hat zu dieser Tabelle alle für eine Tabelle möglichen Rechte, d.h. die Rechte `SELECT`, `INSERT`, `UPDATE`, `DELETE`, `REFERENCES` und `TRIGGER`.

Beispiel:

Angenommen der Benutzer `Admin` hat alle Tabellen der Mondial-Datenbank erzeugt und besitzt somit alle Rechte. Das Leserecht zu der Tabelle `Land` soll dem Benutzer `PUBLIC` erteilt werden Außerdem, sollen den Benutzern `Assistent` und `Tutor` die Rechte zum Lesen, Einfügen, Löschen und Ändern zugeteilt werden in der Weise, dass diese Benutzer diese Rechte auch anderen Benutzer erteilen dürfen. Schließlich soll der Benutzer `SysProg` die Rechte `REFERENCES` und `TRIGGER` erhalten.

```
GRANT SELECT ON Land TO PUBLIC

GRANT SELECT, INSERT, DELETE, UPDATE
ON Land TO Assistent, Tutor WITH GRANT OPTION

GRANT REFERENCES, TRIGGER
ON Land TO SysProg
```

Bemerkungen

- Die Definition von Fremdschlüsseln, Integritätsbedingungen und Triggern darf nur bei Besitz entsprechender Rechte erlaubt sein, da sonst indirekt der Inhalt der Tabelle `Land` geschlossen werden könnte.
- Jeder Benutzer, der ein `SELECT`-Recht zu `Land` besitzt, darf eine Sicht über dieser Tabelle definieren.
- Wird eine Sicht über mehreren Tabellen definiert, dann muss das `SELECT`-Recht zu allen diesen Tabellen zugeteilt sein. Weitere Rechte zu der Sicht existieren nur dann, wenn diese Rechte auch für alle der Sicht zugrunde liegenden Tabellen besessen werden.

zum REVOKE

Ein Recht R heißt *verlassen*, wenn das Recht, das für seine Zuteilung erforderlich war, zurückgezogen wurde und keine weitere Zuteilung von R vorgenommen wurde, deren erforderlichen Rechte noch existieren.

- Die Option `CASCADE` veranlaßt zusätzlich zu der Rücknahme des in der `REVOKE`-Klausel benannten Rechts auch die Zurücknahme aller verlassenen Rechte.
- die Option `RESTRICT` führt zum Abbruch der `REVOKE`-Anweisung, wenn verlassene Rechte resultieren.

Benutzer Assistent teilt dem Benutzer Tutor ein INSERT-Recht für Land zu.

```
GRANT INSERT ON Land TO Tutor
```

Es folgen eine Reihe von durch Benutzer Admin vorgenommene REVOKE-Anweisungen.

```
REVOKE INSERT ON Land FROM Tutor RESTRICT
```

Tutor behält das Recht, da er es unabhängig auch von Assistent erhielt.

```
REVOKE INSERT ON Land FROM Assistent CASCADE
```

Jetzt verliert sowohl Assistent, als auch Tutor das Recht. Angenommen, Admin führt anstatt der letzten Anweisung

```
REVOKE GRANT OPTION FOR INSERT ON Land
FROM Assistent CASCADE
```

aus. Jetzt behält Assistent das INSERT-Recht, jedoch Tutor verliert es, da die Erlaubnis für die Vergabe des Rechts an ihn zurückgezogen wurde.